UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/658,253	09/08/2000	Stefan Nusser	SOM9-2000-0012-US1	3070

23334 7590 05/20/2004

FLEIT, KAIN, GIBBONS, GUTMAN, BONGINI
& BIANCO P.L.
ONE BOCA COMMERCE CENTER
551 NORTHWEST 77TH STREET, SUITE 111
BOCA RATON, FL 33487

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 05/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/658,253	NUSSER ET AL.	
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 4 recites the limitation "the application" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 4-5, 7-9, 10-13, 21, and 27 are rejected under 35 U.S.C. 103(a) as being anticipated by Moore US Patent No 5,343,527 in view of Brown et al US Patent No 4,972,472. Moore discloses a hybrid encryption method for protecting reusable

software components. Brown discloses a method of changing the master key in a cryptographic system.

5. With regards to claim 1, Moore teaches the creating of data K where at least one scheme is based upon the integrity of the module to be verified (Moore, column 9 lines 34-47, column 12 lines 35-61), creating an authentication token for the module which produces K in both schemes (Moore, column 9 lines 34-47, column 12 lines 35-61), using K as created by one scheme to disrupt the module (Moore, column 9 lines 34-47), and using K as created by the other scheme to restore the module (Moore, column 12 lines 35-61). Moore fails to teach a second scheme for determining K that would be used for disrupting the module. Brown teaches a scheme for producing K and using K to disrupt the module (Boesch, column 6 lines 28-45). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Brown's method of producing K with Moore because it offers the advantage of increasing the security of the keys involved in encryption/decryption and minimizing the likelihood that unauthorized persons will be able to break the encryption and access the data (Brown, column 1 lines 26-47).

6. With regards to claim 2, Moore as modified teaches one or more schemes being based on RSA encryption (Moore, column 3 lines 43-48, column 9 line 68 – column 10 line 3).

7. With regards to claim 4, Moore as modified teaches the embedding of a public component of one or more of the schemes in a verification code of the application (Moore, column 12 lines 27-35).

8. With regards to claim 5, Moore as modified teaches the conveying of private components of all schemes to a module authentication authority (Moore, column 10 lines 53-58).

9. With regards to claim 7, Moore as modified teaches the authentication token being embedded in the external module as long as the external module itself remains functional (Moore, Figure 4, column 10 lines 53-58, lines 19-23).

10. With regards to claim 8, Moore as modified teaches a system for allowing developers to submit the hash of their module (Moore, column 10 lines 53-58), but fails to teach a web site allowing the submission. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to allow submission by a web-site with Moore as modified because it offers the advantage of providing a point of submission that is accessible to any internet connected computer because of the widespread use of HTML and web-sites.

11. With regards to claim 9, Moore as modified teaches the authentication token being external to the external module (Moore, Figure 4).

12. With regards to claim 10, Moore as modified teaches the scheme depending on code integrity being independent of a location of the external module in memory (Moore, column 12 line 15 – column 13 line 5).

13. With regards to claim 11, Moore as modified teaches the location independence being achieved by locating and reading the external module's image on a disk (Moore, column 12 lines 35-48).

14. With regards to claim 12, Moore as modified teaches the location independence being achieved using a canonical hash (Moore, column 12 lines 35-48).

15. With regards to claims 13, 21, and 27, Moore teaches the loading of an external module into memory (Moore, column 13 lines 40-55) and the use of a public security code or a public and private component pair for accessings keys (Moore, column 12 lines 27-40), but fails to teach the decrypting of a number of pseudo-random bytes that are part of an authentication token for the STOMPing process. Brown teaches the decrypting of a number of pseudo-random bytes that are part of an authentication token for the STOMPing process (Boesch, column 6 lines 28-45). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Brown's method of producing K with Moore as modified because it offers the advantage of increasing the security of the keys involved in encryption/decryption and minimizing the likelihood that unauthorized persons will be able to break the encryption and access the data (Brown, column 1 lines 26-47).

16. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moore US Patent No 5,343,527 and Brown et al US Patent No 4,972,472 as applied to claim 1 above, and further in view of Ghizzoni et al US Patent No 6,698,016. Ghizzoni teaches a system for injecting code into another process.

17. With regards to claim 8, Moore as modified fails to teach the embedding being realized by adding additional code to a portable executable file. Ghizzoni teaches embedding being realized by adding additional code to a portable executable file

(Ghizzoni, column 7 line 54 – column 8 line 30). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ghizzoni's method of using portable executable files with Moore as modified because it offers the advantage of providing memory locations with clear mappings of the addresses of the file contents (Ghizzoni, column 7 line 61 – column 8 line 8).

18. Claims 15 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moore US Patent No 5,343,527 and Brown et al US Patent No 4,972,472 as applied to claim 13 above, and further in view of Granger et al US Patent No 6,480,959. Granger teaches a system for controlling the use of software programs.

19. With regards to claims 15 and 23, Moore as modified fails to teach the XORing of the decrypted pseudo-random bytes with the external module to make the module unusable. Granger teaches the XORing of the decrypted pseudo-random bytes with the external module to make the module unusable (Granger, column 10 lines 22-29). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Granger's method of encrypting with an XOR with Moore as modified because it offers the advantage of providing a relatively simple encryption algorithm that is low in overhead and thus requires a small amount of computational time (Granger, column 10 lines 22-29).

20. Claims 3, 13-14, 16-19, 22, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moore US Patent No 5,343,527, Brown et al US Patent No 4,972,472, and Granger et al US Patent No 6,480,959 as applied to claim 15 above, and further in view of Dwork et al US Patent No 5,978,482. Dwork teaches a method for protection of digital information.

21. With regards to claims 3, 16, and 24, Moore as modified teaches the using of a hash to begin an UNSTOMP process (Moore, column 12 lines 41-58), but fails to teach the performing of a signet extrication to generate extrication data. Dwork teaches the performing of a signet extrication to generate extrication data (Dwork, column 4 lines 7-14). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Dwork's method of signet extrication With Moore as modified because it offers the advantage of providing a method of preventing the user from sharing keys with illegitimate users (Dwork, column 1 lines 64-67).

22. With regards to claims 14 and 22, Moore as modified teaches the public and private components of the security code comprising security codes from the group of a signet pair (Dwork, column 7 lines 50-66) and an RSA pair (Moore, column 10 lines 1-15).

23. With regards to claim 17 and 25, Moore as modified teaches the using of extrication data to generate another stream of pseudo-random bytes (Dwork, column 7 lines 50-66).

24. With regards to claims 18 and 26, Moore as modified teaches the XORing of another stream of pseudo-random bytes with the unusable external module thereby

making the external module usable in the event that there has been no illicit patching of the external module (Granger, column 10 lines 22-29, Moore, column 12 line 67 – column 13 line 4) and maintaining the unusable external module unusable in the event that the external module has been illicitly patched such that an application or program that is accessing the module fails to operate (Moore, column 12 lines 41-67).

25. With regards to claim 19, Moore as modified teaches the authenticating of the external module by performing the STOMP and UNSTOMP process multiple times (Moore, column 9 line 60 – column 10 line 58 and column 11 lines 15-65). Moore fails to teach the periodic re-authenticating. Granger teaches the periodic re-authenticating (Granger, column 5 lines 10-25). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Granger's method of periodically authenticating with Moore as modified because it offers the advantage of increasing security by halting the application during execution if authentication has failed (Granger, column 5 lines 10-25).

26. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moore US Patent No 5,343,527, Brown et al US Patent No 4,972,472, Granger et al US Patent No 6,480,959, and Dwork et al US Patent No 5,978,482 as applied to claim 18 above, and further in view of Golan US Patent No 5,974,549. Golan discloses a security monitor system.

27. With regards to claim 20, Moore as modified fails to teach the performing of run time checks to make sure that an attacker does not intercept function calls to the

external module. Golan teaches the performing of run time checks to make sure that an attacker does not intercept function calls to the external module (Golan, column 2 line 58 – column 3 line 5). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Golan's method of run time checks with Moore as modified because it offers the advantage of providing a secure system where software components can execute in a secure manner (Golan, column 2 lines 13-28).

Conclusion

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

Andrew Nalven

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137